CAPIRE BITCOIN (ovvero Bitcoin e Criptomonete per Tutti)

La rivoluzione di Bitcoin e delle valute digitali decentralizzate spiegata in un linguaggio semplice, a cura del Bitcoin Veneto Center Team.

Indice (clicca e salti all'argomento che ti interessa):

PREMESSA GENERALE: il mondo delle transazioni economiche – e con esso il mondo intero – sta cambiando, e tale dinamica è certamente legata alla nascita, allo sviluppo, all'affermazione e recentemente alla letterale esplosione della cosiddetta finanza decentralizzata (DeFi), ossia quel sistema che fondendo informatica, tecnologia e teoria del valore e della moneta, nonché basilari concetti della macroeconomia, ha permesso di giungere all'idea – ormai non più fantascientifica – di un meccanismo di scambi economici che risulti libero da intermediazioni centralizzate, con tutto quello che tale concetto comporta in termini di libertà, trasparenza, privacy e autonomia dei singoli attori, ovvero utenti.

Ancora oggi protagonista assoluto di questa rivoluzione, nonché primo in ordine strettamente temporale, è certamente bitcoin (BTC), cioè la prima "criptomoneta" in assoluto (un concetto, quello di "criptomoneta", che ovviamente andremo a spiegare in seguito) ed il relativo Registro Distribuito, la blockchain di bitcoin.

La nascita di Bitcoin risale al 2008, quando, in un'anonima chat per addetti al lavori, il misterioso Satoshi Nakamoto (pseudonimo di una figura ormai entrata nella leggenda, che con tutta probabilità non è mai stato un unico personaggio, ma un team di crittografi, sviluppatori, informatici ed economisti) annunciava al mondo l'aver coniato un sistema P2P (peer to peer, ossia decentralizzato in forma distribuita tra nodi del tutto identici, senza alcun intermediario) in grado di cambiare per sempre le transazioni tra attori economici.

Da gennaio 2009 ad oggi, bitcoin (la moneta si scrive con la "b" minuscola, mentre la sua blockchain è Bitcoin con la "B" maiuscola), valuta completamente digitale e letteralmente "programmata" per mimare il comportamento economico ed il valore di un metallo prezioso (spiegheremo dettagliatamente anche questa pseudo - magia informatica), ha mantenuto tutte le promesse, attestandosi a vero e proprio bene rifugio largamente riconosciuto come tale da un'ormai vastissima comunità di consumatori, imprenditori e istituzioni sia commerciali che finanziarie (nonostante le tante resistenze iniziali da parte di scettici e detrattori e l'alta volatilità del suo valore di cambio).

Il valore di mercato di un BTC ha infatti confermato in pieno le previsioni economiche dei suoi programmatori, ed è per questo che oggi sono in moltissimi a definirlo abitualmente come vero e proprio oro digitale, una riserva di valore capace di coniugare l'idea del più antico mezzo di pagamento e scambio con la velocità ed efficienza delle moderni reti telematiche.

Ma c'è ancora molta strada da fare, specie nel campo dell'educazione a questi nuovi concetti e alla protezione dai tanti portatori di interesse che oggi non vedono di buon occhio la diffusione di un sistema di conservazione della ricchezza e di transazione economica così

indipendente e libero dai tanti limiti e controlli dei sistemi classici (si pensi ai poteri forti in ambito bancario, agli interessi legati ai grandi fondi speculativi, ai ricatti economici connessi ai sistemi monetari e all'inflazione, per citarne qualcuno).

L'informazione mainstream (termine inglese entrato nel vocabolario italiano che significa "corrente principale" oppure "opinione corrente", definendo correntemente i media mainstream come mezzi d'informazione convenzionali o tradizionali quali giornali, radio e TV, in contrapposizione ai cosiddetti alternative media, canali d'informazione nati e fruiti in rete) tende ad essere ancora molto ostile al tema delle criptomonete, sia per banale ignoranza in materia, sia in quanto assoldata da gruppi di persone ed aziende che hanno tutto il vantaggio a tenere per sé precise informazioni, ed i frutti di un monopolio finanziario che rischia di sfuggire loro di mano se "scoperto" e utilizzato dagli utenti profani.

Lo scopo di questa breve spiegazione è anche quello di precisare la vera natura di bitcoin (come anche, ovviamente più in generale, di tutti i numerosi progetti che da esso sono indirettamente derivati), non solo per descriverne i vantaggi e le potenzialità, ma anche per sfatare le tantissime, troppe mitologie oscure che ancora vengono arbitrariamente – e talvolta in malafede – associate a questo nome: la moneta del terrorismo internazionale, delle truffe online, degli evasori fiscali e via discorrendo lungo i canali del complottismo di bassa lega e della falsità bella e buona.

Bitcoin, assieme a svariati altri progetti criptomonetari (in gergo altcoin, moneta alternativa), è al contrario il riferimento di scambio del futuro, la riserva aurea del mondo nuovo, disponibile per tutti attraverso un minimo di formazione di base che possa permettere a chiunque di acquisirlo, detenerlo, conservarlo, scambiarlo e utilizzarlo al meglio, al riparo da rischi e in modo pratico ed efficiente.

ALCUNE NOZIONI DI BASE… COS'È LA MONETA? Ciascuno di noi ha, per forza di cose, un'idea abbastanza precisa di cosa sia la moneta. Questa idea, però, è spesso sbagliata, o meglio giusta e funzionante nella vita quotidiana, ma non precisa a livello di definizione.

Si pensa che la moneta sia sinonimo di ricchezza, ma non è così: insomma, i tanto agognati soldi non sono di per sé "la ricchezza", ma lo strumento per effettuare degli scambi di valore alternativi al baratto, sistema vigente in civiltà che oggi chiameremmo primitive.

Se sono nel deserto e ho centomila euro o una grossa pepita d'oro, non posso dirmi ricco perché in quel contesto euro ed oro non si traducono in asset (entità materiale o immateriale suscettibile di valutazione economica) utili, al contrario di un litro d'acqua, preziosissima.

La moneta, quindi, altro non è che un mezzo che viene accettato come sistema di pagamento di beni o servizi, nonché come modalità per conservare tale valore per utilizzi futuri.

In origine, la moneta – esigenza divenuta assolutamente naturale nel passaggio dalle economie di consumo personale a quelle legate ai commerci ed al risparmio – era quella coniata in metalli preziosi come l'argento e l'oro (cosiddetta hard money, moneta pesante), ossia "materiali" con determinate caratteristiche: immutabilità delle proprietà chimico-fisiche, malleabilità, possibilità di lavorazione (gioielli e monili) con produzione di oggetti facilmente frazionabili e trasportabili (per esempio i lingotti), oltre alle vere e proprie monete.

Con lo sviluppo dei traffici per terra e per mare e il perfezionamento del sistema bancario, la moneta aurea è stata progressivamente affiancata dalla cosiddetta paper money, moneta cartacea, ossia un "contratto", che inizialmente aveva la funzione di attestare l'esistenza, per esempio, di una certa riserva d'oro (o terreni, o proprietà), che chiaramente non poteva essere trasferita portandola con sé in un viaggio.

In origine, questa moneta era un banale pezzo di carta firmato al cospetto di un'autorità e attestava l'esistenza di una certa ricchezza in un certo luogo (quindi di un concetto anch'esso hard, pesante, oggettivo e concreto).

Con l'andare del tempo, questi "contratti" si sono trasformati, ovvero standardizzati in produzione seriale, nella moneta che conosciamo oggi.

Una banconota da venti dollari o dieci euro altro non è, se ci pensiamo, che un "contratto standard stampato con numeri di serie differenti" che afferma che il portatore del medesimo è possessore di venti dollari o dieci euro.

Caratteristica fondamentale di questa particolare forma di moneta è la fungibilità, nel senso che il valore attribuito a cinque banconote da dieci euro possedute da Tizio è esattamente identico al valore della banconota singola da cinquanta euro posseduta da Sempronio. La fungibilità consente tutte le operazioni matematiche necessarie per misurare la ricchezza, comunicarla, gestirla, trasferirla e in tal modo darle senso.

Altra caratteristica importantissima della paper money è che viene emessa per definizione da una precisa autorità superiore, che abbiamo imparato a identificare nelle grandi banche centrali nazionali, come la Federal Reserve per il dollaro statunitense o la BCE per l'euro.

L'unico tassello che ci manca è il passaggio da paper money a cosiddetta fiat money…

Fino alla fine degli anni Sessanta, la moneta "cartacea" (o metallica non preziosa) è stata emessa sempre sulla base di precise riserve d'oro detenute dalle banche centrali, ovvero dalle autorità monetarie nazionali.

Erano esattamente queste riserve – che in economia si dicono "collaterali" o "sottostanti" – a sancire l'autorevolezza e conformemente la validità nazionalmente riconosciuta della moneta stessa, che diventava vera e propria valuta, garanzia del potere economico dello stato emettitore.

Questo aspetto, cioè la validità territoriale-statuale, è vigente anche oggi ma con una differenza: dal 1971 le politiche monetarie statunitensi – poi estese al resto del mondo – hanno definitivamente sganciato la stampa (anche informatica, in quanto solo il 10% circa della valuta in circolazione è cartacea, il restante 90% sono numeri e stringhe di codice nei computer delle Banche) dall'esistenza fisica di un collaterale in oro, inaugurando l'era della fiat money, ossia della moneta emessa in termini che potremmo dire "fiduciari" sull'esistenza di attività economiche nazionali in grado di giustificarla (il PIL di una nazione).

La moneta diventa in questo caso un *pagherò* sulla fiducia, una scommessa sugli andamenti economici globali (con tutti i problemi che tale formula può anche intuitivamente evidenziare).

Riassumendo, oggi il denaro "comune" con cui siamo abituati ad avere a che fare ogni giorno è letteralmente un pezzo di carta o una stringa di "bit", emesso in serie dalla banca centrale relativa al territorio nel quale operiamo, che per legge deve essere accettato in tutto quel territorio in quanto oggetto fungibile che veicola un valore oggettivo decretato come ufficiale.

In altre parole, se mi reco in un ristorante o in un supermercato, in Italia o in Europa, e pago in euro, la cassa non può assolutamente rifiutarsi di accettarli come sistema di pagamento (se pago in noccioline, o con un lingotto d'oro, il gestore può accettare questi sistemi di pagamento, come tanti altri, ma non è obbligato a farlo).

INTERMEZZO: QUALI SONO I PROBLEMI DELLA MONETA FIAT MONEY? Una delle più note teorie economiche sul valore ha a che fare con la scarsità.

Il concetto è semplice: un'aragosta a Santo Domingo può costarmi come un caffè a Roma, per il semplice fatto che la quantità di torrefazioni romane è infinitamente superiore alla quantità di aragoste che posso trovare a Roma.

Se una “cosa” è abbondante, vale di meno.

Che l’oro sia un metallo raro e prezioso lo dice la storia e il buonsenso, ma sia la storia che il buonsenso esprimono un dato di fatto oggettivo: i giacimenti d’oro non sono infiniti, e l’oro risulta infinitamente più scarso del ferro e dei comuni metalli.

La possibilità di stampare moneta senza alcun limite introduce il concetto di inflazione, ossia di aumento indiscriminato di valuta nel mercato e se questa azione può risultare funzionale a politiche monetarie e macroeconomiche di breve periodo, nel lungo periodo essa produce gli effetti ben noti della svalutazione, che in certi casi può assumere una portata disastrosa per l’economia di un paese.

Di recente (2014/2020) il Venezuela ha attraversato una delle peggiori congiunture economiche di sempre, dovuta alla svalutazione del Bolivares, moneta nazionale diventata praticamente senza alcun valore rispetto al dollaro.

Curioso – anche se di questo parleremo dopo – che sia stato proprio un progetto “criptomonetario” a sollevare la nazione attraverso l’azione della DASH Foundation, che ha diffuso nel paese bancomat ATM “cripto” in grado di cambiare in DASH i pochi dollari circolanti, mantenendo il potere d’acquisto, utilizzabile per pagare i beni e servizi più disparati, dal trasporto pubblico al pranzo in un fast food.

A parte gli effetti di fenomeni svalutativi poderosi come quello venezuelano, l’inflazione relativa alla cartamoneta costituisce, a detta di numerosi e illustri economisti, la dinamica che porterà inevitabilmente, sia pure per gradi e con parziali assestamenti intermedi, al declino, o al forte ridimensionamento, del sistema finanziario e monetario basato sulla fiat money.

Esattamente sulla base di questa considerazione si è mosso bitcoin, introducendo dall’origine il concetto di una moneta la cui offerta massima fosse collegata ad attività della rete “programmate” per remunerare i suoi attori di riferimento (i cosiddetti miners, minatori, di cui parleremo più avanti) con una produzione di criptovaluta limitata fin dall’inizio ad un massimo di 21 milioni di monete, con inflazione programmata.

In altre parole, bitcoin è stato progettato per mimare il comportamento dell’oro anche in un contesto immateriale e intangibile come quello digitale ed in questo senso, l’espressione “oro digitale”, spesso usata nel gergo, diventa ancora più comprensibile, soprattutto se consideriamo che tutte le promesse di Satoshi Nakamoto si sono puntualmente avverate: la crescita in valore del BTC è stata – a meno di fluttuazioni fisiologiche, nonché di picchi

episodici – costante fino al raggiungimento oggi di livelli da vero e proprio bene rifugio.

MA LE CRIPTOMONETE SONO VERAMENTE MONETE? Una delle principali critiche alle criptomonete come sistema di pagamento è legata da un lato al fatto di non essere emesse da una banca centrale (mancanza di obbligatorietà di accettazione tranne in El Salvador, prima nazione ad annunciare di aver promosso a valuta di Stato il bitcoin, affiancato al dollaro USA, nel giugno 2021), e dall'altro alla volatilità di mercato, che le renderebbe poco adatte a conservare il valore per utilizzi immediati o differiti (come abbiamo visto, caratteristica basilare della moneta).

Queste critiche sono discutibili, per vari motivi, ma tralasciando gli effetti dell'inflazione, ossia considerando per un attimo le "monete classiche" come effettivo strumento di conservazione della stabilità di una certa ricchezza (cosa, come detto, tutt'altro che scontata), c'è da dire che numerosi beni a valore fluttuante – basti pensare alle azioni di borsa, alle quotazioni di note aziende multinazionali, per non parlare del valore di immobili e terreni – sono comunemente impiegati come valore di scambio, l'unica difficoltà è come ovvio la spendibilità spicciola, visto che difficilmente qualcuno andrebbe a comprarsi un caffè o a fare la spesa pagando con un sacchetto di terra o un'azione borsistica, anche se potesse, ma la moderna tecnologia permette già oggi di avere a disposizione portafogli digitali (in gergo, il wallet) in grado di farci usare le criptomonete per comprare anche la spesa o un pieno di benzina cambiandole in Euro per poi caricarli in una comune carta di debito Visa o Mastercard collegata al proprio wallet.

La questione della velocità di transazione è tale da trasformare di molto lo scenario nel quale giudichiamo un tale asset – in questo caso, appunto, digitale o digitalizzato – più o meno valevole come strumento di scambio, ossia moneta.

Dal punto di vista funzionale, essendo che la moneta ha come principale caratteristica quella di essere tutto ciò che viene comunemente accettato come sistema di pagamento, questo

basterebbe a rispondere esaurientemente alla critica, dato che la velocità di transazione permette di effettuare un cambio immediato e pagare direttamente in "asset" di varia natura, comprese le criptomonete.

Una risposta merita anche l'obiezione relativa alla volatilità, visto che questa caratteristica è certamente propria delle criptomonete in generale, ma non di tutte dato che esistono delle particolari tipologie di monete (in gergo, coin) e di gettoni (in gergo, token), le cosiddette stablecoins o monete stabili, progettate per garantire valore fisso pari ad un dollaro o un euro.

Si tratta di vere e proprie criptomonete, che però, o attraverso la presenza certificata di opportuni collaterali fisici (in valuta, o in metallo prezioso), oppure attraverso complessi algoritmi automatizzati e sincronizzati con la liquidità e il circolante, consentono di mantenere tutti i vantaggi della decentralizzazione pur avendo un controvalore monetario assolutamente stabile e fisso.

Quanto alla mancata emissione da parte di autorità centrali e nazionali, questa sembrerebbe più una caratteristica positiva che negativa dato che il bitcoin è una moneta assolutamente internazionale, legata a un sistema di produzione e scambio (che più avanti descriveremo) del tutto distribuito, delocalizzato e decentralizzato.

La battuta può essere un po' truce, ma va pronunciata: per distruggere il sistema eurocentrico basterebbe distruggere gli stabilimenti tipografici della Banca Centrale Europea, le tipografie/zecche informatiche BCE; per distruggere bitcoin bisognerebbe distruggere tutte le migliaia e migliaia di computer dislocati sull'intero pianeta, sopprimendo tutti i nodi che ne permettono il funzionamento decentralizzato. Possibile, certo, ma altamente improbabile.

Oltre a questo, più avanti vedremo come bitcoin sia non solo paritetico, ma per molti versi addirittura preferibile alla moneta per ragioni di libertà ed emancipazione dagli intermediari finanziari classici, dalle loro regole spesso opache e restrittive, e non da ultimo dal rischio che spesso e volentieri veicolano indirettamente (si pensi ai periodici crack finanziari di istituti che sembravano solidissimi).

Se a questo aggiungiamo ulteriori vantaggi, come le basse commissioni per le transazioni, la trasparenza, la facilità d'uso con semplici App per smartphone, telefonini e computer, l'assenza di terze parti tra noi e il destinatario, il quadro è completo ed è un quadro largamente a favore di bitcoin, delle criptomonete e della tecnologia sottostante.

IL BITCOIN SOTTO IL COFANO: COSA SI INTENDE PER DECENTRALIZZAZIONE E IL RUOLO DELLA CRITTOGRAFIA: il cuore di qualsiasi discorso sulle criptomonete non può prescindere, come detto, dal concetto di decentralizzazione ma questo concetto deve essere approfondito aggiungendo alcuni dettagli.

Se immaginiamo infatti una qualsiasi idea intuitiva di "moneta digitale", dobbiamo necessariamente fare riferimento a una verità di fondo, che probabilmente l'utente medio ignora, o non considera: tutto ciò che è digitale – e a maggior ragione tutto ciò che transita digitalmente per le reti telematiche che abbiamo imparato a riconoscere come internet – altro non è che informazione.

Dai comuni euro che trasferiamo attraverso un bonifico effettuato con l'applicazione smartphone della nostra banca, agli stessi BTC trasferiti attraverso dispositivi quasi del tutto analoghi (i cosiddetti wallet di prima, di cui parleremo), definiscono la stessa cosa: un trasferimento di informazioni da A a B (peer 2 peer o P2P, paritario/paritario).

L'informazione può trasmettersi attraverso architetture informatiche molto diverse tra loro: le architetture centralizzate sono quelle tipiche anche del sistema bancario e finanziario classico, con un "nodo centrale" che si collega a tutti gli altri nodi periferici, potendoli controllare e smistando tutta l'informazione che transita.

Se il sig. A volesse inviare al sig. B una somma di denaro attraverso un comune bonifico, ossia facendo riferimento al suo IBAN, stiamo indirettamente alludendo a questo schema sequenziale centralizzato: A invia una certa informazione di pagamento alla Banca di A (primo nodo centralizzato), la quale contatta la Banca di B (secondo nodo centralizzato), affinché trasferisca tale informazione di pagamento al conto di B.

Come vedi, ben quattro nodi sono stati coinvolti in questa transazione, pur essendo solo due i soggetti implicati.

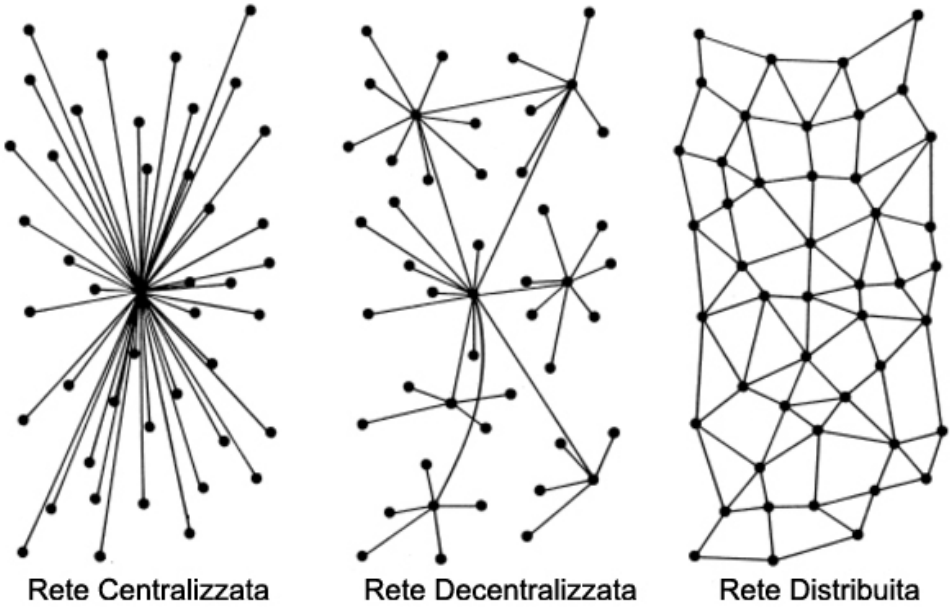
In questo ultimo esempio si suppone che tali "nodi centrali" fungano anche da controllori della transazione e che forniscano garanzie in caso di attacco informatico, o di assicurazione in caso di perdita dei fondi, e via discorrendo.

Di contro, i medesimi possono però anche sindacare sull'operazione, bloccarla, indirizzare altrove i fondi, ed altre amenità.

Se immaginiamo invece un sistema decentralizzato, dove una transazione digitale di fondi (che

come abbiamo detto è pura informazione) passi da A a B senza alcuna mediazione di ulteriori nodi, allora dobbiamo necessariamente prevedere un sistema che metta tale informazione al riparo da eventuali soggetti indesiderati che possano intercettarla, alterarla, e dunque manometterla.

Qui sotto un'immagine delle tre tipologie di reti possibili: centralizzata, decentralizzata e distribuita (quella che usa bitcoin).



La parola magica che l'informatica (ossia la teoria dell'informazione che è una branca della matematica) mette a disposizione per risolvere questo problema è la crittografia, ossia un sistema che permette all'informazione che transita da A a B di "acquisire senso leggibile" solo una volta giunta a destinazione.

In un sistema decentralizzato in modalità P2P (peer to peer), ossia in un sistema distribuito dove ciascun nodo può entrare in contatto con qualsiasi altro, le parole d'ordine dell'architettura crittografica in grado di gestire l'informazione in modo assolutamente sicuro e al riparo da manomissioni esterne sono due: **chiave pubblica** e **chiave privata**.

Immaginiamo un oggetto – esclusivamente in nostro possesso fisico – in grado di "contenere" (il termine è improprio, ma lo usiamo per facilitare la comprensione) delle "monete digitali" (bitcoin, per esempio); chiameremo questo oggetto il wallet (in inglese, portafoglio).

Immaginiamo di voler inviare tali monete, o una parte di esse, a un nostro amico, detentore di un wallet simile al nostro.

Ebbene, il singolo wallet è un dispositivo che permette di "firmare" con quella che noi chiamiamo chiave privata, ossia una sequenza alfanumerica complessa che solo noi dobbiamo poter conoscere e usare, in quanto ci consente di essere appunto gli unici "decisori" delle transazioni in uscita da quel wallet.

La chiave privata è un'informazione particolare che attraverso opportuni meccanismi algoritmici monodirezionali (spiegheremo poi perché) crea la chiave pubblica, che è un'ulteriore stringa alfanumerica complessa – logicamente diversa dalla chiave privata – che noi utilizziamo non per inviare, ma per "farci inviare" fondi al nostro wallet.

In altre parole, la chiave pubblica funziona esattamente come una specie di IBAN "cripto", che noi comunichiamo tranquillamente ad amici o clienti che vogliano inviare i loro BTC al nostro wallet (si dice "pubblica" perché possiamo farla conoscere a chiunque, visto che la sola cosa che può succedere è che qualcuno ci invii dei fondi criptomonetari).

Capiamo facilmente il perché la generazione algoritmica della chiave pubblica dalla chiave privata sia un processo a una sola direzione: se qualcuno potesse ricostruire la chiave privata a partire da quella pubblica, ossia in senso inverso, questo significherebbe per lui avere pieno accesso, tramite un comune wallet "riprogrammato", ai nostri fondi, ovvero alla loro gestione.

Ecco perché la crittografia è strettamente legata all'idea di sistema distribuito, ed ecco perché le "criptomonete" si chiamano così: non perché ci sia di mezzo la kryptonite, o perché la cosa – come dicono ancora molti giornalisti del mainstream che intendono divulgare un giudizio su bitcoin e affini senza però sapere minimamente cosa siano – abbia a che fare col Dark Web, l'internet oscuro o altre cose occulte e misteriose.

La parola "cripto" allude quindi solo all'unico modo efficace per garantire la piena sicurezza di transito in un mondo fatto di pura informazione, o per meglio dire, di impulsi composti da infinite sequenze di bit trasmessi da dispositivi connessi in rete.

Ecco perché, la prossima volta che parlerete a qualcuno di criptomonete, capirete che non state parlando di "moneta occulta", ma di "moneta sicura".

I MINATORI, QUESTI SCONOSCIUTI. Ma in che modo funziona il sistema che permette il funzionamento di bitcoin, se "la rete" altro non è un sistema di "nodi connessi", laddove per

nodi intendiamo certamente dei soggetti, ma tecnicamente degli “oggetti” identificabili di volta in volta da precisi dispositivi tecnologici, in primis computer, nonché analoghi elaboratori? Un ruolo indubbiamente centrale e particolare è quello rivestito dai cosiddetti “minatori” (in gergo, i miners).

Questi nodi, lungi dall’essere entità di centralizzazione, sono immaginabili come dei soldati semplici, o per meglio dire delle infaticabili formiche operaie, disperse nella rete stessa e abilitate a svolgere delle funzioni molto particolari – comunque equamente retribuite – al fine di sostenere esistenza, efficacia, efficienza e sicurezza della rete stessa e delle sue transazioni.

Semplificando, i minatori sono costituiti da una serie di computer partecipanti alla rete che entrano in competizione per essere gli unici a cui è consentito registrare tutte le transazioni recenti e, se il computer è in grado di vincere la competizione, può aggiudicarsi un po’ di bitcoin “nuovi” come ricompensa.

Questi calcolatori risolvono complessi puzzle computazionali, quindi il mining di bitcoin è assolutamente necessario per mantenere il registro delle transazioni su cui si basa bitcoin.

Quando i computer miner risolvono problemi matematici sulla rete bitcoin, estraggono nuovi bitcoin (non diversamente da quando un’operazione classica di un minatore estrae oro da una miniera), rendono contestualmente la rete di pagamento bitcoin affidabile e sicura, verificando e cristallizzando le informazioni sulle transazioni.

I miner hanno compiti particolari, che sintetizzando e semplificando al massimo, vengono affidati sulla base di un criterio algoritmico di implementazione e protezione chiamato proof-of-work (in gergo la PoW o letteralmente, prova da lavoro) e costituiscono la base assoluta di funzionamento di tutta la rete di transazioni.

Il concetto di proof-of-work, per quanto tecnicamente complesso, è facilmente comprensibile nella sua sostanza funzionale, perché si tratta di disincentivare rigorosamente determinate dinamiche di attacco al sistema (per esempio quello che noi possiamo riconoscere nello SPAM della posta elettronica) costringendo il nodo a svolgere dei “lavori” piuttosto complicati dal punto di vista computazionale, ma comunque fattibili ed entro un intervallo di tollerabilità costo-beneficio, il cui esito possa essere rapidamente controllato dal sistema stesso attraverso una rapida “prova del nove” algoritmica.

Nel caso del sopraccitato spam, oggi comunque riconosciuto da sistemi che lo aggirano in modalità diverse (esempio, parole chiave che alludono a offerte commerciali indesiderate,

discrepanze di traduzione, ed altri indizi), una minimale proof-of-work potrebbe essere rappresentata dall'obbligo di effettuare un semplice calcolo algebrico prima di spedirci una qualsiasi mail.

Più comunemente, alcuni siti richiedono, prima di entrare, o durante l'autenticazione, di risolvere semplici puzzle, o di dimostrare la propria "umanità" attraverso il riconoscimento visivo di elementi all'interno di un'immagine, i cosiddetti chaptcha.

Nel caso dei miners, la proof-of-work prevista dal "sistema Nakamoto" permette di risolvere contemporaneamente tutta una serie di condizioni di base del sistema, affidando ai medesimi tre funzioni fondamentali:

- la validazione delle transazioni, attraverso un plurimo controllo delle cosiddette stringhe hash (in sostanza, stringhe alfanumeriche di output che dimostrano, se confrontate e prive di errori, la non-manomissione di una certa informazione di transazione);
- l'accorpamento delle transazioni in cosiddetti "blocchi" (da cui il termine blockchain, che andremo a descrivere tra poco), sulla base di criteri di efficacia ed efficienza stabiliti a priori in modalità automatizzata;
- una funzione di automatica remunerazione ai miners stessi, in forma di vera e propria produzione di nuovi bitcoin, nonché di redistribuzione delle cosiddette commissioni di rete, ossia frazioni di bitcoin che vengono spese dagli utenti per godere di certe performance della rete stessa, come la velocità della conferma della transazione da immettere in blockchain.

Più nel dettaglio, i miners sono super-computer che vengono premiati su base (per così dire) "meritocratica" in ragione del lavoro che svolgono per mantenere sicura e fluida la rete, ossia macchine che svolgono procedure a intenso carico computazionale, direttamente legato alla quantità di transazioni da processare, al peso in bit delle transazioni stesse, alla logica di "impacchettamento" in blocchi che saranno eseguiti prima o dopo nell'unità di tempo, all'efficacia ed efficienza di implementazione sulla base di standard stabiliti dall'algoritmo.

Una caratteristica piuttosto interessante è rappresentata dal criterio di remunerazione da produzione ex novo di criptomoneta, che nel caso dei miners segue una logica perfettamente calata nella coerenza originaria del modello Sakamoto: la limitazione superiore dell'ammontare complessivo di bitcoin producibili.

L'intero sistema, quindi, converge a un futuro dove il bitcoin circolante sarà fisso, e l'attività dei miners – già opportunamente retribuiti per il lavoro svolto – andrà a coprire le funzioni di

base (logicamente meno onerose in termini di performance hardware) della validazione e dell'efficienza in blockchain, con un livello remunerativo di base stabilizzato.

LA BLOCKCHAIN. Eccoci dunque a definire quella catena di blocchi che costituisce forse una delle espressioni più sentite in gergo "cripto" (ma non certamente la più chiara).

In realtà si tratta di un concetto molto semplice: la blockchain è il registro elettronico distribuito e decentralizzato che annota tutte le transazioni di bitcoin (o di altre criptomonete, con blockchain dedicate) avvenute nei relativi wallet identificati dalle chiavi pubbliche ad essi riferiti, e in tal modo visionabili da chiunque in modo assolutamente trasparente.

Questa stessa semplice definizione ci permette di sfatare un altro mito, secondo il quale bitcoin sarebbe una moneta oscura e imperscrutabile, mentre vale l'esatto contrario: un IBAN non permette certo di visionare il saldo e i movimenti del relativo conto; una chiave pubblica, invece, lo permette eccome, attraverso il registro blockchain.

L'unica differenza è che l'uso di bitcoin prevede l'identificazione di stringhe alfanumeriche, che non riportano assolutamente i dati anagrafici di chi detiene le relative chiavi private: si tratta, quindi, non tanto di un sistema anonimo, ma di un sistema semi-anonimo o pseudonimo, il cui grado di riservatezza è gestibile a piena responsabilità dell'utente, che sceglierà in autonomia a chi comunicare la proprietà di una determinata chiave pubblica.

La blockchain funziona appunto attraverso sequenze di blocchi che contengono – in senso ovviamente informatico – i dettagli identificativi di tutte le transazioni, ordinate secondo criteri che vanno dal grado di remunerazione in termini di commissioni di rete, alla quantità di valuta trasferita, alla modulazione di velocità di trasferimento richiesta dall'utente attraverso le varie opzioni del wallet, e altre variabili secondarie.

La modalità blockchain è anche stata usata in campi non direttamente connessi alle transazioni economiche, o comunque non esclusivamente ad esse legati.

Su questi sistemi "girano" ormai numerose funzioni, come quelle legate a particolari criptomonete come ETH nella rete Ethereum, che vanno dalla validazione documentale alle firme digitali, dalla gestione di veri e propri siti (il nostro test bitcoinveneto.cripto) a funzioni di comunicazione criptata (mail, chat), fino allo scambio di cosiddetti NFT (Non Fungible Tokens), ossia "oggetti digitali" a tiratura singola o limitata, che vanno a riprodurre perfettamente l'atto di proprietà in formato "digitale" di un'opera d'arte o da collezionismo.

Quest'ultima frontiera (settore peraltro in crescita esponenziale), avente a che fare soprattutto con il cosiddetto smart contract (contratto intelligente) consente di svolgere una vastissima gamma di funzioni, che arrivano a estendere la finanza decentralizzata anche a servizi un tempo implementabili solo attraverso l'intermediazione "umana" di operatori, banche, finanziarie e affini: mutui e prestiti decentralizzati, mining indiretto attraverso vincolo a tempo di somme di criptomoneta, etc.

BITCOIN IN CONCRETO: IL WALLET DIGITALE. Per gestire la normale cartamoneta utilizziamo un portafoglio, per moneta digitale come un conto bancario in Euro usiamo App di home banking, e per gestire la criptomoneta utilizziamo un portafoglio digitale, in inglese wallet, che altro non sono se non dei software che "girano" all'interno di un device digitale, sia esso un computer fisso o portatile, oppure un'App per smartphone o tablet.

A titolo di esempio, un wallet digitale (qualsiasi) è scaricabile da un comune App Store – i sistemi più diffusi sono quelli per Android e iOS – e utilizzabile in un qualsiasi smartphone.

All'apertura, il wallet ci chiede se vogliamo creare un nuovo wallet, oppure se intendiamo utilizzarne uno già di nostra proprietà. Il concetto di "proprietà" è legato alla conoscenza di una frase seme (seed phrase) – solitamente di dodici o ventiquattro parole – che in pratica costituisce il cuore del wallet e che attraverso un procedimento matematico - algoritmico andrà a generare le coppie di chiavi pubbliche/private necessarie al funzionamento delle relative criptomonete attivabili in quel wallet (ogni criptomoneta ha uno specifico – chiamiamolo – "cripto iban" dedicato a quel "tipo" di moneta).

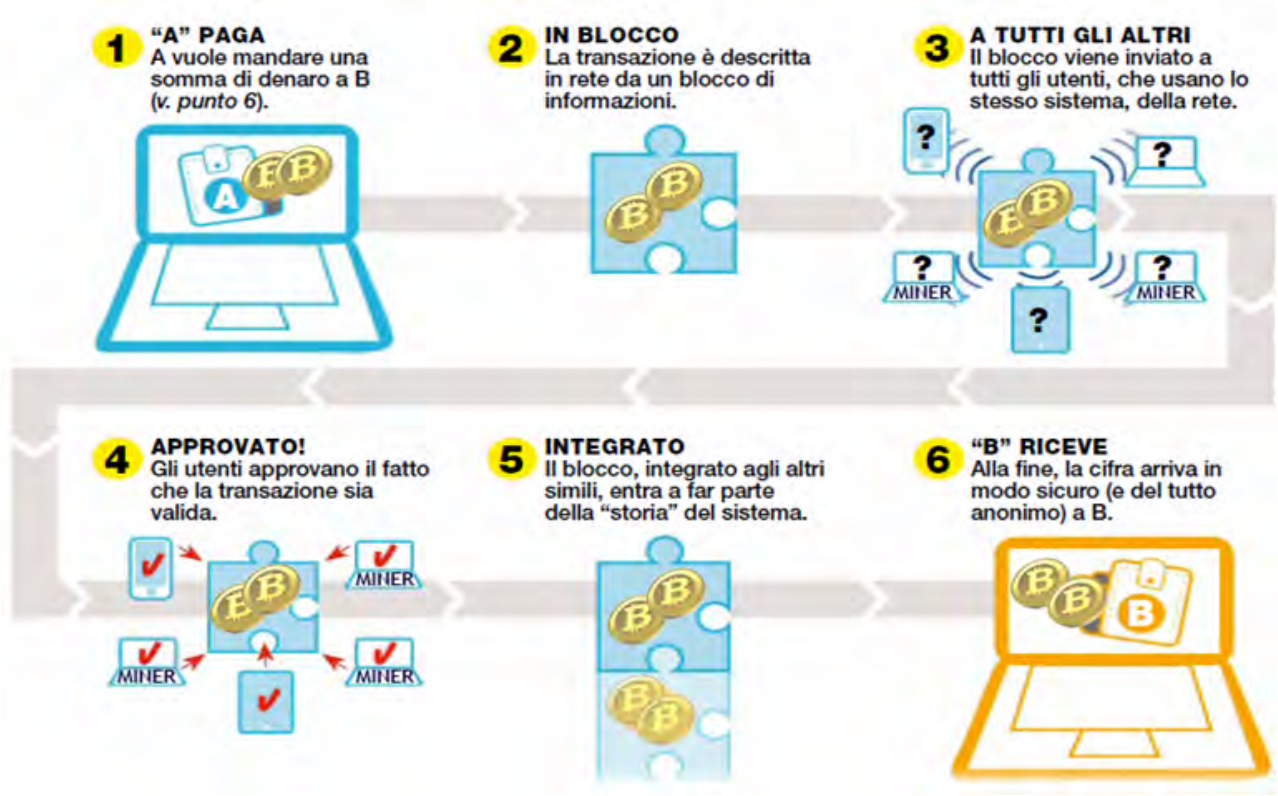
Supponiamo di non conoscere alcuna frase segreta, e di voler aprire un "conto cripto" del tutto nuovo. I moderni wallet ci consentono di generare automaticamente e casualmente una stringa crittografata (solo noi la conosceremo) che viene immediatamente tradotta in una sequenza di parole. Il wallet ci chiederà di annotare queste parole su carta, di nasconderle e custodirle con estrema attenzione visto che solo quelle ci permetteranno di recuperare i fondi inviati nel wallet, in caso di perdita, furto, rottura del device, etc...

Una volta effettuata questa operazione e una volta confermata nel wallet (che di solito chiede di inserire la frase a ulteriore conferma), siamo pronti a usare il wallet stesso (che probabilmente, avendo memorizzato la chiave privata al suo interno, ci chiederà di aggiungere anche una comoda password personale, un PIN o l'uso dell'impronta digitale al fine di impedire l'uso dell'App a terzi parti, come in una comune applicazione di home banking).

Siamo pronti dunque a ricevere criptomoneta e inviarla ad amici, parenti e clienti che abbiano un wallet simile il nostro, chiaramente con i loro indirizzi di chiave pubblica. Oltre a questo, siamo anche pronti a spendere criptomoneta in tutti quei siti web – o anche negozi fisici, in Italia ad oggi 2021 poco meno di mille, mappa on line su quibitcoin.it/cerca-su-mappa – che la accettano come mezzo di pagamento.

Supponiamo ora di avere un amico che ci vuole spedire dall'estero, o comunque da una certa distanza, un bitcoin (l'ipotesi è piuttosto rosea, visto che il bitcoin, mentre scriviamo ha raggiunto un valore di varie decine di migliaia di euro, e dunque – a meno che non abbiate un amico particolarmente generoso o che vi deve una parcella piuttosto corposa – è più probabile che il vostro amico vi spedisca una "frazione" di bitcoin, ovvero una manciata di cosiddetti satoshi, la frazione più piccola di bitcoin, che ne rappresenta un centomilionesimo).

Come avviene la transazione? Tutto è molto semplice. Il vostro wallet genera una stringa corrispondente alla vostra "chiave pubblica in BTC", che voi dovete comunicare al vostro amico esattamente come un comune IBAN. Il vostro amico, copierà e incollerà questa sequenza di lettere e numeri nello spazio apposito del suo wallet, deciderà quanto inviarvi, stabilirà eventualmente alcune variabili aggiuntive (magari una commissione un po' più alta per invogliare la rete a confermare la transazione più rapidamente) e darà il via alla trasmissione. L'informazione di invio verrà "impacchettata" in un blocco di transazioni dal sistema che abbiamo descritto in precedenza e dopo opportuna validazione multipla stabilita dal sistema stesso vedrete l'accredito direttamente nel vostro wallet. Ora avete anche voi bitcoin (frazioni di BTC, satoshi) nel vostro wallet e potete fare esattamente la stessa cosa avendo a disposizione le chiavi pubbliche di utenti come voi.

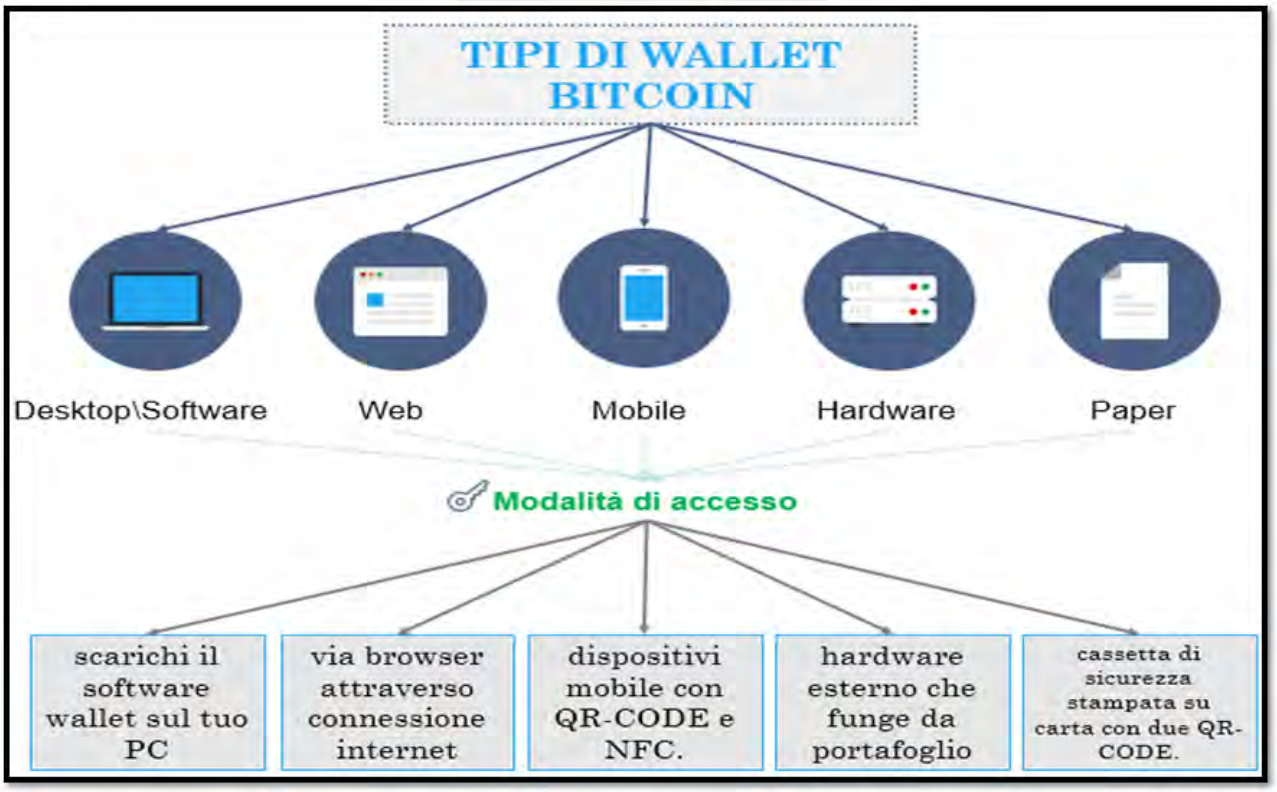


Se invece siete faccia a faccia con la persona da cui dovete ricevere (o cui volete inviare) BTC, un modo più semplice del "copia e incolla" è il QR code, immagini molto simili ai comuni codici a barre che velocizzano anche la spesa al supermercato tramite lettori ottici alle casse.

Un QR code altro non è che un tipo diverso di codice a barre che può contenere, se letto dall'apposita App lettore, fino a 4.000 caratteri alfanumerici, quindi siti web, indirizzi email ma anche chiavi pubbliche, evitando eventuali errori di digitazione (difatti vengono ormai usati come standard per comunicare per esempio il sito ufficiale di un certo brand, evitando complesse digitazioni). Insomma, l'invio di criptomoneta tramite i QR code è un gioco da ragazzi. Basta inquadrare, digitare l'importo, confermare l'operazione con PIN o impronta digitale e inviare.

Nota bene: Per completezza è giusto dire che alcune particolari criptomonete – come Ripple o gli Stellar Lumens – prevedono oltre all'indirizzo (chiave pubblica) anche una sorta di "causale" (il cosiddetto memo) che necessariamente deve essere allegato alla transazione per giungere al destinatario. I moderni wallet, comunque, avvertono sempre della necessità di aggiungere queste particolari causali, che di solito si limitano a brevi stringhe numeriche che possono essere tranquillamente aggiunte a mano.

Differenti tipi di wallet: custodial e non-custodial. Il wallet che abbiamo appena descritto è quello che maggiormente viene utilizzato per detenere una certa quantità di criptomoneta, di relativo controvalore in valuta FIAT. Si tratta di un wallet che letteralmente "ingloba la chiave privata" senza alcuna terza parte implicata. Un adagio molto noto nel campo cripto recita: not your keys not your coins… Se non sei tu a possedere le chiavi (private) non sei tu a possedere la criptomoneta. Cosa significa? Vediamolo nel dettaglio.



Un wallet del genere è detto non-custodial, espressione che sta per "portafoglio non-custode", cioè nessuno a parte noi custodisce la chiave privata.

Questo genere di wallet permette di gestire le criptomonete in modalità completamente decentralizzata. A meno che qualcuno riesca a sbirciare il foglietto rigorosamente cartaceo dove abbiamo annotato le parole della seed phrase, nessuno è in grado di gestire i nostri soldi.

Tuttavia esistono dei servizi online – quasi sempre grossi Exchange (piattaforme dove acquistare e scambiare criptomoneta online) – che ci forniscono particolari wallet dove sono loro a gestire le chiavi private al nostro posto. Questi wallet si dicono appunto custodial, cioè custodi.

Perché mai far gestire ad altri le informazioni che sono alla base della decentralizzazione pura? Non abbiamo forse parlato di una vera e propria rivoluzione legata alla possibilità di essere noi stessi la nostra banca? Non sta forse nella totale assenza di intermediari il vero cuore pulsante di queste innovazioni? Certo, ma andiamo per gradi.

Il grande sviluppo della criptomoneta, nonché l'esplosione del suo valore, mappato da siti ufficiali che sono diventati ormai una vera e propria "cripto borsa", ha chiaramente prodotto delle dinamiche finanziarie estremamente appetibili, che oggi permettono a grandi fornitori di servizi di offrire numerose funzioni all'utente base, medio o esperto.

Effettuare un servizio di "custodia chiavi private" consente a tali soggetti di accedere a interessanti economie di scala, e dunque di erogare "in cambio" tantissimi servizi aggiuntivi: trading online, mining indiretto, sconti sull'acquisto di criptomoneta, servizi di cashback connessi alla messa in vincolo (cosiddetto staking, statico o flessibile) di determinate classi di criptomonete, veri e propri interessi pagati giornalmente, settimanalmente, mensilmente o annualmente, servizi annessi all'emissione di carte di debito in grado di spendere criptomoneta anche nei classici circuiti Visa o Mastercard, funzioni bancarie e chi più ne ha più ne metta.

La scelta di un wallet custodial non è dunque una follia, ma un rischio ponderato sulla base di vantaggi aggiuntivi che per alcuni utenti possono valere la candela. A tale proposito, noi addetti al lavori consigliamo sempre di essere paranoici, ma non troppo. Più nello specifico, il wallet non custodial risulta adatto a detenere cifre importanti, mentre quello custodial viene solitamente utilizzato per trasferire quantità più esigue, o comunque percepite dall'utente come ragionevoli per attivare determinati servizi di interesse (anche se, in effetti, servizi di custodia di ingenti patrimoni, come l'italiano Checksig.io offrono anche un'assicurazione su quanto messo in custodia, fondi sempre disponibili ed altri servizi utili).

Parlando dunque di scelta del wallet, i consigli sono essenzialmente due: diversificare per quantità e tipologia. In altre parole, scegliere il wallet sulla base dell'entità del suo contenuto, e nel contempo evitare di mettere tutto in un solo posto. Ovviamente questi consigli variano a seconda dell'utente. Per alcuni una cifra di mille euro può essere considerata irrisoria, per altri può essere invece notevole.

Dove e come acquistare criptomonete? *(NOTA: all'interno di questa piccola guida troverete dei link a prodotti o servizi commerciali, che abbiamo usato o usiamo personalmente e che riteniamo validi. I link sono collegati al nostro reflink, un codice personale che ci riconosce piccoli bonus, sconti o micro percentuali su acquisti e uso di servizi che effettuerete passando attraverso*

questi collegamenti pubblicitari "speciali". Qualunque servizio o prodotto userete o acquisterete tramite questi reflink non aggiungeranno costi di nessun tipo, sono una sorta di mancia che ci viene riconosciuta per lo sforzo di valutare ed includere i vari servizi, dopo averli testati o utilizzati, nella guida stessa.)

Eccoci dunque al tema che, nella pratica, interessa di più: dove posso comprare (o meglio cambiare) criptomonete contro Euro?

Escludendo per ora l'attività di mining, per ovvie ragioni destinata a personale esperto, addetti ai lavori in ambito informatico, oltre che persone che necessariamente devono dotarsi di strutture di calcolo piuttosto costose e dalla complessa manutenzione, ed essendo i settori che "pagano in cripto" piuttosto rari, nonché confinati a progetti specifici di carattere informatico, il solo modo per avere criptomoneta è, ragionevolmente, comprarla.

I cosiddetti Exchange sono i soggetti che trattano questo tipo di prodotto. Attraverso molti comuni sistemi di pagamento, come bonifici ma anche in contanti, carta di credito o debito, abbiamo a disposizione una vasta gamma di operatori che possono farci arrivare – o direttamente all'indirizzo del nostro wallet oppure in un conto (in inglese, account) da aprire previa registrazione nell'exchange stesso – tutta la criptomoneta che desideriamo.

Tra i molti Exchange presenti sul web noi consigliamo l'italianissimo TheRockTrading.com, il più vecchio Exchange al mondo (anche se di dimensioni medio-piccole ma con sede legale in Italia), lo statunitense Kraken (che ha avuto recentemente la certificazione bancaria da parte dell'autorità statunitense) ed infine Binance (uno dei più grandi esistenti legato al mercato soprattutto asiatico ma in espansione mondiale).

Il consiglio che però ci sentiamo di porgere all'utente medio è di valutare attentamente la sua conoscenza pregressa, prima di rivolgersi direttamente a questi siti. Sembrerà una banalità, ma è chiaro che – traduzioni a parte – questi operatori fanno capo a società che comunicano in inglese (a parte TheRockTrading.com), che gestiscono l'assistenza clienti attraverso mezzi del tutto telematici, spesso automatizzati, e che propongono servizi la cui complessità andrebbe affrontata con un minimo di esperienza.

Chi, banalmente (e legittimamente), non sa da dove iniziare, dovrebbe rivolgersi a operatori locali, meglio se centrati fisicamente nel territorio con sedi fisse e regolari aziende di consulenza e formazione. Questi operatori, oltre a parlare in italiano e ad avere un rapporto diretto col cliente, sono abilitati a fornire direttamente servizi di compravendita – che per determinate cifre possono avvenire in contanti, con regolare fattura a norma di legge – in

modo da facilitare e velocizzare di molto ogni transazione.

Il vantaggio di un "consulente di fiducia" è chiaramente legato alla possibilità di rivolgere domande e ottenere risposte senza attese. Oltre a questo, un consulente può dimensionare e cucire su misura il servizio a seconda delle precise e uniche esigenze di ciascuno, evitando le standardizzazioni che per forza di cose devono essere implementate in un servizio automatizzato e "freddo" come quello fornito a schermo da un sito internet.

Q&A: Domande e risposte frequenti + Critiche (e Confutazioni)

Bitcoin è una moneta anonima? Sì e no. La verità è che bitcoin, come quasi tutte le criptomonete, è definibile come moneta semi-anonima o pseudonima, in quanto si basa su un registro blockchain che annota in modo assolutamente trasparente ogni transazione.

Le transazioni, però, non fanno capo a "nomi e cognomi", ma a stringhe alfanumeriche che denotano wallet e trasferimenti tra i medesimi. Se non non sappiamo a chi appartiene una certa chiave pubblica, ovviamente non possiamo sapere a chi appartiene un certo saldo evidenziato in blockchain.

Se però una persona o istituzione dichiara apertamente – esattamente come può accadere per un comune IBAN – la sua chiave pubblica, allora noi possiamo tranquillamente vedere a quanto ammonta il suo saldo e quali sono i movimenti del suo conto.

Tutto, insomma, dipende dalla volontà del possessore delle chiavi private: Bitcoin è sinonimo di libertà e responsabilità personale.

Bitcoin è impignorabile, insequestrabile? Se dicessimo di no, diremmo una sostanziale bugia dato che la correttezza etica e fiscale impone di dichiarare eventuali depositi in criptomoneta, ma non sono molti gli studi di commercialisti che trattano abitualmente la questione, in modo del tutto trasparente e normato.

Di fatto, però, una qualsiasi transazione (non solo bitcoin) effettuata attraverso wallet di tipo non-custodial, non può assolutamente essere fermata da mano umana (come può accadere per un comune bonifico bancario), e molto a fatica un giudice riuscirebbe "tecnicamente" a vincolare un deposito di bitcoin aperto a titolo personale, visto che:

1. dovrebbe comunque conoscerne l'esistenza – cosa tutt'altro che banale, visto che il possessore potrebbe aver aperto un nuovo wallet anche pochi minuti prima, trasferendo tutti i suoi bitcoin da un altro wallet, magari pure conosciuto;

2. dovrebbe imporre con la forza al medesimo possessore di rivelare la frase segreta, ovvero la chiave privata (o SEED).

Come detto, la criptomoneta ha a che fare con la libertà finanziaria e l'assenza di intermediari e coercizioni; come in ogni cosa, la bontà o malvagità di uno strumento non sta nello strumento, ma in chi lo usa.

Esistono criptomonete totalmente anonime? Sì, esistono delle particolari criptomonete dette privacy-coin (come Zcash e DASH in via opzionale, oppure Monero in via standard, solo per citarne alcune) che, attraverso meccanismi algoritmici molto particolari risultano totalmente oscurabili agli occhi di terzi o in altre parole, facendo un esempio concreto, se Tizio rivela al mondo la sua chiave pubblica bitcoin, chiunque può tranquillamente andare a controllare il suo saldo e i movimenti ad esso relativi, tramite un semplice esploratore della blockchain (blockexplorer, a questo link un esempio Blockchair.com).

Se Sempronio rivela al mondo la sua chiave pubblica in una moneta come Monero, non esiste un modo semplice di rintracciare il saldo o i movimenti, visto che il registro della relativa blockchain di quest'ultima coin è visibile solo a livello di wallet personale.

Dove è possibile spendere Bitcoin e criptomonete? Ormai sono numerosi i portali che consentono di acquistare direttamente, attraverso opportuni QR code "cripto" che registrano immediatamente la transazione, numerosi prodotti e servizi: buoni carburante delle maggiori compagnie, carte regalo da spendere in catene commerciali (librerie, supermercati, negozi di abbigliamento, elettronica, viaggi, trasporti, etc…), ricariche spendibili nei più noti e-commerce (primo tra tutti Amazon, che non ha bisogno di presentazioni a livello merceologico) e ricariche telefoniche; una mappa italiana delle attività commerciali con sede fisica si può vedere nel sito www.quibitcoin.it

Oltre a questo, sono numerosi i servizi che consentono di trasferire criptomoneta a comuni carte di debito e ricaricabili che effettuano automaticamente una conversione in moneta locale e consentono di pagare in qualsiasi esercizio commerciale abbia a disposizione un comune apparato POS, o di prelevare contante in una postazione ATM e se a questo aggiungiamo la crescita esponenziale dei commercianti ed esercenti che accettano pagamenti cripto, arriviamo certamente a dire che ormai la criptomoneta è spendibile ovunque.

Il valore di Bitcoin crescerà veramente nel tempo? Esistono prove della crescita del potere di acquisto di Bitcoin? Sì, molte.

In materia, un dato statistico molto interessante è quello che confronta l'andamento decennale dell'ammontare di dollari necessari all'acquisto di un hamburger di McDonalds o di una tazza di latte di Starbucks rispetto alla quantità di bitcoin per acquistare i medesimi prodotti.

Ne risulta chiaramente che – dal 2011 al 2021 – l'andamento del dollaro è costantemente crescente (ossia, ne servono sempre di più, quindi vale sempre di meno), mentre quello di bitcoin è all'opposto costantemente decrescente (ossia ne servono sempre di meno, quindi ha un potere di acquisto in costante crescita).

Bitcoin è un asset digitale, che come qualsiasi altro asset, anche non digitale, può aumentare o diminuire di valore (cosa che accade praticamente ogni secondo, con estrema volatilità nel brevissimo periodo), sulla base della ben nota interazione tra domanda e offerta.

Curioso notare come ci si preoccupi tanto del valore di bitcoin, che nel tempo ha dato prova oggettiva di mantenere ogni promessa legata alla sua valorizzazione connessa alla "programmata scarsità" (da cui l'espressione "oro digitale") e non ci si preoccupi invece della lenta ma costante svalutazione di euro e dollaro, e di tutte le altre valute nazionali, per non parlare del mercato borsistico, che arricchisce molte persone pure nelle sue fluttuazioni.

I media mainstream spesso e volentieri descrivono bitcoin come una bolla effimera, che nel futuro crollerà di valore, non si sa bene perché, ma gli stessi media, però, tacciono costantemente sui fenomeni di iper-inflazione che oggi come oggi stanno letteralmente annientando il potere d'acquisto delle monete tradizionali per ottenere materie prime fondamentali per la produzione industriale e di beni di prima necessità.

La domanda è dunque un'altra: ragionando sui settori che oggi trainano l'economia globale, se avessimo dovuto investire qualcosa vent'anni fa, avendo magicamente la possibilità di farlo "col senno del poi", dove saremmo andati a mettere i nostri soldi?

In un'azienda come Amazon, che ha fatto delle vendite online (tecnologia a suo tempo definita pure quella come una bolla passeggera) la sua ricchezza determinante, oppure in una comune azienda di costruzioni?

In altre parole, cosa sarà più valido e ricercato in futuro? Il tanto amato mattone, un pezzo di carta stampato da una banca centrale oppure un asset ad alta tecnologia?

A dirla con una battuta, ci fu qualcuno che ebbe a dire che nessuno avrebbe mai passato le sue serate davanti a una scatola con uno schermo che trasmetteva stupide immagini in movimento… questo per dire che sono svariati i settori di successo che inizialmente sono stati considerati delle mode passeggere, per non dire delle follie.

Si legge in internet che il mondo delle criptovalute è pieno di truffe. Questa affermazione, più che falsa, è assolutamente decontestualizzata e parziale dato che le truffe che avvengono con le criptomonete sono infinitamente meno di quelle fatte con dollari ed euro.

Per ogni hacker che è riuscito a prelevare qualche moneta cripto in qualche exchange, o per ogni utente che per sbaglio ha comunicato la sua chiave privata a terzi rispondendo incautamente a una mail, ce ne sono almeno dieci che hanno violato comuni carte di credito e conti correnti. Quindi, come spesso accade, spesso si tratta di notizie messe in giro e amplificate per mettere in cattiva luce una novità che potrebbe dare fastidio a qualcuno, banche e società finanziarie centralizzate in primis.

Ma la verità, almeno dal nostro punto di vista e con dati attendibili, è l'esatto opposto: non potrebbe esistere luogo più sicuro di un wallet non-custodial conservato con cura per detenere e vedere crescere i propri risparmi, al riparo dagli artigli dell'inflazione e degli intermediari.

Cosa si intende per operazione Over The Counter (OTC)? Quante volte, specie di fronte all'annuncio della vendita di una grande villa o di un immobile prestigioso, abbiamo visto la dicitura di trattativa privata?

Si tratta quasi sempre di trattative che riferiscono a un prezzo di vendita che per ragioni di "tutela del mercato" non può essere comunicato a terzi, ma solo a chi effettivamente è interessato all'acquisto (evidentemente di un bene che necessita di un esborso piuttosto corposo in termini monetari).

In altre parole, supponiamo che la villa in questione abbia un prezzo di mercato di un milione di euro ed il proprietario, però, intende vendere subito o in tempi molto rapidi, quindi è ragionevolmente disposto a fare uno sconto notevole, diciamo di duecentomila euro.

Se si sapesse che quella villa è acquistabile a ottocentomila euro, probabilmente l'intero mercato andrebbe al ribasso, mentre nel caso di trattativa privata il mercato resterebbe intatto, l'acquirente farebbe un affare e chi vende avrebbe monetizzato sulla base delle sue aspettative.

Una cosa del genere avviene anche nel mondo cripto, attraverso operatori specializzati che si occupano di far avvenire la compravendita secondo il principio dell'incontro tra la domanda e l'offerta soltanto, al di fuori dei mercati tradizionali; perciò il valore del tasso di cambio potrà essere decorrelato rispetto all'andamento del tasso dei normali exchange.

L'acronimo OTC allude esattamente a queste operazioni, a "negoziazione diretta".

Bitcoin potrebbe essere censurato da banche centrali o da Governi? Tecnicamente, questa cosa è impossibile perché per "censurare" bitcoin bisognerebbe annientare tutti i suoi nodi, quindi, come minimo (anche se non basterebbe), smantellare l'intera rete Internet, con tutti i disastri che questo comporterebbe per gli stessi soggetti che volessero intraprendere tale azione, qualora fattibile.

Peraltro, lo stesso smantellamento della rete web globale non basterebbe, visto che i nodi potrebbero continuare a funzionare attraverso connessioni alternative (satellitari, radio, intranet, direttamente da smartphone a smartphone, etc...).

Più banalmente, bitcoin non è che "informazione pura trasmessa in modalità crittografica", quindi uno smantellamento o una censura risulterebbero difformi da qualsiasi normativa vigente in materia di libertà, almeno nella quasi totalità dei paesi occidentali.

In altre parole, prima di censurare bitcoin dovrebbero censurare preventivamente ogni forma di comunicazione personale, di proprietà intellettuale, di protocollo per le normali attività di connessione tramite chat, mail, videoconferenza. Il tutto, per ottenere cosa?

Una normativa calata dall'alto può colpire i grandi exchange? Premesso che i bitcoin possono essere ottenuti attraverso procedure alternative al puro acquisto "in negozio", e che comunque esistono vari metodi alternativi all'Exchange per effettuare l'acquisto stesso (come i Dex, Exchange decentralizzati), la proibizione di vendere bitcoin avrebbe lo stesso senso della proibizione di vendere figurine di comuni calciatori, o monili, o opere d'arte, qualora dovessero iniziare a valere molto.

Risulta difficile ammettere la possibilità che una "normativa", cioè di una disposizione per sua definizione "legata al diritto", vada a stabilire una prassi contraria allo stesso diritto che l'ha generata e la rende possibile.

Peraltro, ciò che sta accadendo è l'esatto opposto, dato che grandi Exchange stanno ottenendo lo status di vere e proprie banche (Kraken), nonché soggetti quotati in borsa (Coinbase), con

un riconoscimento istituzionale crescente e condiviso.

Se a questo aggiungiamo l'aumento di soggetti istituzionali che accumulano bitcoin come collaterale e bene rifugio (a giugno 2021 El Salvador ha adottato bitcoin come moneta di scambio nazionale), nonché in molti casi anche come base speculativa, ci rendiamo conto che uno scenario di attacco agli Exchange risulta opposto alla tendenza storica.

Gli hacker diventeranno sempre più bravi e neppure i Bitcoin saranno al sicuro: se questa affermazione viene presa per vera, allora, come minimo, si dovrebbe proprio correre a comprare bitcoin, visto che qualunque altra applicazione centralizzata in grado di gestire denaro è altrettanto "centralmente" assoggettata al rischio di attacchi informatici e relativi furti.

Invece basta aprire un qualsiasi giornale per rendersi conto di quanto siano praticamente quotidiani i ricorsi alla polizia postale per recuperare somme indebitamente sottratte da conti correnti e carte di credito.

Bitcoin funziona con wallet di cui si possiede in prima persona la chiave privata e l'unico modo che un hacker ha di sottrarre dei fondi in bitcoin consiste nel ricavare o nel farsi comunicare tale chiave privata, che non può essere, matematicamente parlando, ottenuta in alcun modo attraverso procedure algoritmiche.

In altre parole, la cassaforte che contiene i nostri bitcoin può essere aperta solo con una chiave, e quella chiave siamo solo noi (o dovremmo essere solo noi) a detenerla.

Mentre una comune sequenza numerica da carta di credito può essere intercettata e conseguentemente usata da terzi senza il nostro consenso (ecco perché sono sempre più utilizzati i sistemi 3Dsecure che ci chiedono conferma anche tramite SMS o applicazioni dedicate nel nostro smartphone), le transazioni da noi "firmate" in un certo wallet sono monodirezionali, crittate, non modificabili e non censurabili.

Il grado di sicurezza di bitcoin è infinitamente superiore a quello di qualsiasi altra transazione effettuata con metodi classici, digitali o meno e se gli hacker diventeranno bravissimi, di certo bitcoin sarà molto più al sicuro di tanti altri sistemi di conservazione del valore.

I Bitcoin sono la moneta del terrorismo e degli affari loschi: dicerie del genere prescindono completamente da una statistica seria e seriamente comunicata al vasto pubblico.

La diffusione attuale dei bitcoin, se questo fosse vero, individuerebbe affari piuttosto magri per questi traffici, visto che truffe, riciclaggi e compravendite illegali ben più diffuse e corpose viaggiano da decenni, e continuano a viaggiare, in euro e dollari, senza che nessuno abbia nemmeno ipotizzato di bandire queste monete.

Bitcoin è uno strumento di conservazione e scambio di valore, punto e basta, il suo uso, etico o non etico, dipende come in ogni cosa dall'utilizzatore, e non certo dalla tecnologia sottostante.

Peraltro, lo stesso uso di bitcoin come moneta "presunta anonima" è altamente sconsigliabile per chi voglia effettivamente "non essere tracciato", visto che tutte le transazioni sono registrate in blockchain e visibili a chiunque effettui una ricerca sui movimento e sul saldo della data chiave pubblica.

Insomma, la questione della "moneta losca" è semplicemente una narrazione di chi, più o meno in malafede, vuole denigrare bitcoin a prescindere, senza conoscerlo.

Bitcoin è lento rispetto a un comune bonifico immediato: a parte che la rapidità o la lentezza in blockchain è data da una serie di variabili e di impostazioni in parte modificabili a seconda delle esigenze dell'utente, la differenza sostanziale tra un bonifico e una transazione in bitcoin sta nella decentralizzazione.

La battuta, in questo senso, è brutale: provate a farvi inviare da un vostro amico (sempre che abbiate un amico in grado e disposto ad evadere una richiesta del genere) una cifra di trecentomila euro tramite bonifico, e vedrete due cose che, con molta probabilità, accadrebbero in rapida sequenza; la prima, parcheggio del bonifico in entrata da parte della banca; la seconda, telefonata del direttore che vi tempesterà di domande sull'origine dei fondi, sulla motivazione della transazione, sull'ordinante del bonifico, e chi più ne ha più ne metta.

Non accade nulla, invece, nel caso di un invio di tot bitcoin per l'equivalente della cifra sopraccitata: il vostro amico ve li invia, e voi li ricevete. Punto.

Ma è vero che Bitcoin danneggia l'ambiente per il suo dispendio energetico? Questa bufala è legata, ovviamente da rapporti manipolati ad hoc, all'attività connessa alla proof-of-work (miners) in termini di dispendio energetico connesso alla performance computazionale, mentre in realtà è stato calcolato che la sommatoria di tutti i computer "lasciati accesi per nulla" con la spia dello stan-by, solo in USA supera del 60% l'intero ammontare dell'energia consumata dalla rete bitcoin.

Se poi confrontiamo l'impatto ambientale della medesima con quello delle comuni caldaie vetuste, che caratterizzano ancora la schiacciante maggioranza dei comuni immobili di tutta Italia, ci rendiamo conto di come il vero inquinamento sia dato dalla mancata riconversione ecologica, e non certo dall'attività di mining (che peraltro, come descritto altrove, è stata progettata per essere sempre minore, fino a un livello di base assolutamente irrisorio).

Ormai è tardi per acquistare Bitcoin, non me lo posso permettere: falso, in assoluto, perché se da un lato è vero che certi "minatori fedeli" (o anche compratori della prima ora) si sono ritrovati milionari nel giro di quattro o cinque anni, è anche vero che la storia di bitcoin risulta ancora ai suoi primi passi, specie se consideriamo il crescente interesse da parte di soggetti a 360 gradi nel campo istituzionale.

Bitcoin, se cresce di valore, cresce tutto, sotto-unità comprese e per quanto sia sconsigliato da un punto di vista meramente economico per ragioni di "fees" (commissioni), esistono exchange che consentono anche di acquistare poche decine di euro di bitcoin (mille "satoshi" equivalgono, alla data del presente documento, a circa cinquanta centesimi di dollaro), e di accumulare gradualmente.

Il fatto che un solo bitcoin sia arrivato a picchi di cinquantamila euro e oltre rappresenta uno scoglio puramente "psicologico" e non "sostanziale", visto che l'adozione di bitcoin a livello globale sta crescendo, di fatto, solo ora, e dunque l'innalzamento della domanda a parità di offerta finale porterà a una crescita ulteriore *(quest'ultima affermazione è assolutamente personale e non deve pertanto essere intesa in alcun modo come consiglio operativo di investimento né come sollecitazione alla raccolta di pubblico risparmio).*

Io i miei soldi preferisco tenerli in banca: l'amore dell'italiano medio per lo "sportello" è noto da tempo, anche se piuttosto ingiustificato se consideriamo la storia neppure tanto recente del sistema bancario.

Se siamo dipendenti statali, il cui unico stipendio è pagato dallo Stato già comprensivo di decurtazioni pensionistiche e contributi, allora è certo che un comune e banale conto in banca sia sinonimo, se non di rivalutazione nel tempo (anzi), almeno di sicurezza.

Sta di fatto però che numerose banche fino a poco tempo fa considerate sicure e potenti hanno in questi anni animato le cronache per i loro crack finanziari, inevitabilmente finiti a danno di tantissimi risparmiatori, ma oltre a questo, da almeno quarant'anni a questa parte la storia delle più note e blasonate sigle bancarie del nostro paese porge una continua sequenza di trasformazioni, fusioni, cambiamenti di proprietà e complesse operazioni che di fatto hanno

cancellato nomi un tempo sulla bocca di tutti.

Bitcoin, su questo è opportuno intendersi, non vuole essere contro le banche, ma per una finanza decentralizzata "alternativa" alle sole banche, ossia per la facoltà di scegliere e differenziare il proprio portafoglio finanziario. Ciò che conta, alla fine, è la realtà storica.

La sola verità è che se i tanti che hanno affidato i loro risparmi a determinati e ben noti soggetti del mondo bancario, poi finiti in tribunale per aver piazzato prodotti spazzatura, avessero scelto di acquistare anche solo nel 2015 un equivalente anche solo di tremila euro in bitcoin, oggi si ritroverebbero con un controvalore di circa cinquecentomila euro, e non in causa con una banca che non restituirà loro il becco di un quattrino.

Se consideriamo che i soldi richiesti da questi soggetti per acquisire, appunto, la loro spazzatura, di certo risultavano ben superiori ai citati tremila euro, sia il lettore a trarre le sue conclusioni soppesando il tutto, se è vero che comunque, nel mercato, ancora esistono istituzioni bancarie sufficientemente sicure e affidabili, è anche vero che il "sistema bitcoin" risulta per definizione operativa e strutturale il più sicuro e affidabile (per gli amanti dello sportello e del contatto umano a tutti i costi, comunque, c'è da dire che servizi come quelli forniti dai bitcoin center - in Veneto il Bitcoin Veneto Center di Abano Terme - uniscono la componente tecnologica e quella umana, conservando il meglio di entrambe).

E se arrivasse una criptomoneta migliore di Bitcoin? Questa domanda espressa in forma di critica è sbagliata in quanto tale, perché la presenza di criptomonete "migliori" di bitcoin è in realtà pienamente e attualmente rappresentata da un termine preciso, altcoin (criptomonete alternative), che non mettono minimamente in discussione il valore di bitcoin, ma più banalmente si "specializzano" in funzioni specifiche, alternative a quelle di oro digitale.

Lo stesso sviluppo e la stessa crescita di valore di determinati progetti "criptomonetari" risultano fortemente connessi a bitcoin, che a tutt'oggi delinea gli andamenti dell'intero mercato e pertanto, apprezzare una determinata moneta "alternativa" a bitcoin per qualche specifica ragione (velocità, micropagamenti, facilità d'uso, privacy, etc.) non significa assolutamente denigrare bitcoin, ma solo immaginare di detenere riserve alternative, per scopi altrettanto alternativi.

Di fatto, comunque, c'è da dire che, indipendentemente dall'elevato successo di numerosi progetti "cripto" sia passati che presenti, solo da metà 2021 alcuni progetti sono riusciti, a spot, a superare la supremazia di capitalizzazione di bitcoin, che è rimasto in cima.

In molti parlano di Bitcoin come di una bolla passeggera. In molti parlavano di Amazon come di un modello di business che non poteva reggersi, ma oggi Jeff Bezos, presidente di Amazon, è tra gli uomini più ricchi del pianeta; la stessa cosa si diceva di bitcoin, che nel giro di una scarsa decina d'anni è passato da un valore di pochi dollari a oltre cinquantamila.

I fondi che sempre più istituzioni accumulano in bitcoin non sembrano proprio confermare l'idea di una bolla, ma il suo esatto contrario.

D'altra parte, lo stesso Satoshi Nakamoto (enigmatica figura alla base della nascita di bitcoin, che probabilmente non è neppure una persona, ma un team) ha progettato bitcoin perché fosse come l'oro: un bene a offerta limitata, ovvero con un tetto massimo di "produzione".

Questa intuizione è stata proverbiale: il valore di bitcoin, al netto delle fisiologiche fluttuazioni, continua a salire, rompendo ogni mese il record del mese precedente.

Ma è difficile usare la criptomoneta? Che competenze servono? In realtà usare la criptomoneta è molto più semplice da fare che da spiegare, dato che tutti noi abbiamo ormai a disposizione uno smartphone, Android o Apple che sia.

Ebbene, esistono semplici applicazioni che trasformano lo smartphone in un comune "wallet (portafoglio) digitale", caricabile con le criptomonete che desideriamo.

Un wallet di questo genere funziona esattamente come un lettore di codici a barre (QR-code), del tutto simili a quelli che oggi vengono usati per aprire siti in modo rapido senza dover digitare l'intero indirizzo.

Che si tratti di inviare criptomoneta ad un amico per pagare la propria quota in un regalo di gruppo, o di farsela inviare, o di pagare un prodotto nel web o direttamente in negozio, la procedura è la stessa: inquadrare il codice, digitare la somma o semplicemente acquisirla in caso sia inclusa nel codice stesso, confermare l'operazione attraverso un proprio PIN o codice di sicurezza e inviare il tutto a destinazione.

Dopo poco – in certi casi addirittura in pochi secondi – la transazione sarà completata, il tutto senza bisogno di bonifici, banche, finanziarie e altri intermediari, e se consideriamo le più diffuse applicazioni di home banking, che possono girare sia su computer che su smartphone, sono tantissime le persone del tutto inesperte di informatica che le utilizzano giornalmente, senza porsi problemi di sorta.

Ebbene, queste applicazioni, che come detto vengono manovrate giornalmente da utenti del tutto comuni, ivi compresi anziani, porgono funzioni che in generale sono più complesse di quelle relative a un semplice wallet bitcoin.

Per utilizzare un comune "conto" bitcoin basta semplicemente sapere come si fa ad usare una telecamera per inquadrare un QRcode (facciamo la stessa cosa al supermercato quando inquadriamo un prezzo), oppure, in alternativa, sapere come "copiare e incollare" un certo codice (chiave pubblica) che non si ha voglia e tempo di ricopiare a mano (cosa che sconsigliamo caldamente di fare, per evitare errori).

Peraltro, esistono già oggi delle app che permettono di inviare bitcoin utilizzando sequenze molto più semplici da ricordare (tipo mariorossi.payqualcosa), oppure veri e propri nomi utente, che col tempo diventeranno sempre più diffusi.

Con un minimo di pratica, chiunque può diventare esperto senza alcuna particolare preparazione o attitudine pregressa (il Bitcoin Veneto Center fornisce anche consulenza e corsi base in materia, forniti da operatori esperti e completamente a disposizione del cliente, anche il più "negato" in materia.)

Dal punto di vista fiscale, cosa possiamo dire delle criptomonete? Tutti pensano che bitcoin sia una sorta di cuccagna per evasori e affini, mentre in realtà questa è una mitologia alimentata da chi non conosce la materia.

La blockchain (il registro che annovera tutte le transazioni in cripto) è quanto di più trasparente possa esserci in materia di trasferimento di valore, di conseguenza oggi come oggi esistono prassi semplicissime per dichiarare al fisco i propri fondi criptomonetari, e qualsivoglia operazione poco trasparente condotta in cripto, oltre ad essere più complessa, non ha alcuna differenza rispetto alle medesime, condotte magari in classica valuta nazionale, in trust svizzeri o in paradisi fiscali, la sola differenza sta nell'etica e nella correttezza del singolo, tutte variabili che non riguardano minimamente il mezzo utilizzato, ma chi lo utilizza.

Ma i bitcoin sono sicuri? Perché si dovrebbero scegliere rispetto ad un conto in banca? La finanza "centralizzata" è legata a un complesso costrutto sia economico che istituzionale perché i soldi che noi letteralmente "prestiamo" ad una banca sono nostri finché tutto va bene, ma diventano "molto meno nostri" quando si verifica qualcosa che può direttamente o indirettamente ledere i nostri diritti sui medesimi.

Che si tratti di una ex moglie o di un ex marito capace di pagare avvocati prestigiosi per

pretendere da noi alimenti oltremisura, oppure di una banca che versa in cattive acque (si pensi anche solo a istituti come Banca Etruria e in Veneto la Popolare di Vicenza), oppure di un socio che è scappato con la cassa e ha lasciato a noi tutti i debiti da pagare, oppure decine di altre fattispecie, la prima cosa che farà la banca sarà impedirci di accedere ai nostri fondi.

Ebbene, questa cosa, con bitcoin, è tecnicamente impossibile perché solo noi, grazie alla conoscenza di quella che in gergo si chiama "chiave privata", possiamo disporre dei nostri soldi e quindi, a livello di sicurezza, un wallet cripto è certamente molto, molto più sicuro di qualsivoglia conto corrente.

Che dire allora degli hacker? Non si sono verificati grandi attacchi informatici che hanno svuotato fondi in criptomoneta? Questo è vero, ma si tratta di eventi molto particolari e isolati, che hanno riguardato non già singoli wallet privati, ma precisi Exchange che detenevano le chiavi private dei clienti e funzionavano, in sostanza (anche se tecnicamente l'espressione non sarebbe del tutto corretta) come "cripto banche".

C'è però da dire che questi Exchange, ossia "siti di acquisto cripto", non erano leader nel loro settore, in quanto i "top Exchange" sono perfino più sicuri dei vari siti di home banking ed investono grosse somme per la propria (e dei loro clienti) cybersicurity, investimenti largamente giustificati dagli ingenti movimenti di valuta criptomonetaria che li caratterizza nella loro attività quotidiana.

Oltre a questo, le procedure di sicurezza degli Exchange più solidi (citiamo l'italianissimo TheRockTrading.com, con il quale collaboriamo da anni) non sono confrontabili con quelle di progettualità più giovani o start up in fase di avvio.

In altre parole, un attacco può tecnicamente verificarsi ai danni di qualsiasi Exchange (o istituto bancario), ma si tratta di una possibilità remota e molto improbabile perché, in generale, al di fuori degli Exchange, un furto di cripto può avvenire solo se l'utente comunica inavvertitamente la sua chiave privata a terzi.

La prescrizione è dunque semplice: usare gli Exchange solo come piazze di scambio, effettuare le operazioni necessarie e poi tornare a tenere le proprie cripto sempre in wallet in possesso solo nostro.

Ma quindi? Cosa deve fare una persona che non sa nulla di Bitcoin per entrare in questo mondo? Certamente non fare di testa propria, in quanto la criptosfera può essere piena di

opportunità, ma anche piena di insidie, legate al gran parlare che se ne fa e agli ovvi tentativi truffaldini che molti cercano di mettere in piedi per monetizzare ai danni del malcapitato e ingenuo di turno.

Prima cosa, dunque, rivolgersi a persone esperte e referenziate nel settore, per ricevere dai medesimi una consulenza personalizzata e una buona formazione di base e, successivamente, privilegiare dove possibile il contatto diretto, in sedi fisiche e con persone in carne ed ossa.

Il grosso delle truffe, cripto e non, gira necessariamente sul web, quindi è utile evitare invii di denaro a coordinate bancarie che ci arrivano per posta elettronica, o peggio comunicazione di dati privati e sensibili.

Logicamente esistono moltissimi siti seri e qualificati che trattano la materia, ma è buona cosa approcciarli solo dopo l'apprendimento di alcune nozioni di base, fondamentali per poi muoversi con sicurezza.

Concludiamo questo breve scritto con il link **Bitcoinveneto.it/link-utili** che rimanda al nostro sito divulgativo, interessante da seguire per iniziare, o per approfondimenti e novità, oltre ad invitarti a rivolgerti con fiducia al Bitcoin Veneto Center di Abano Terme per qualsiasi ulteriore dubbio o informazione, dove potrai ricevere consulenza e strumenti operativi per soddisfare ogni tua curiosità ed esigenza personale e professionale!

Visita **Bitcoinvenetocenter.it** per vedere orari e sede, Ti aspettiamo presto;-) **Grazie**.